WEST

Help | Logout | Interrupt

Main Menu | Search Form | Posting Counts | Show S Numbers | Edit S Numbers | Preferences | Cases

Search Results -

Terms	Documents
L11 and l10	0

Database:
US Patents Full-Text Database
US Pre-Grant Publication Full-Text Database
JPO Abstracts Database
EPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L12

Refine Search

Recall Text | Clear

Search History

DATE: Monday, December 23, 2002 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L12	L11 and l10	0	L12
reviewed L11	(attach$ with (product or goods or item) with electronic$ with (label$ or tag$ or indicia)) and @ad<=19980413	30	L11
L10	L9 and (product$ with authentic$)	3	L10
L9	l8 and "decryption key"	23	L9
L8	scan$ and (manufact$ with (product$ or goods or item$)) and (decrypt$ with key$) and @ad<=19980413	76	L8
L7	L4 and (manufact$ with (product$ or goods or item$))	5	L7
L6	L4 and (manufact$ same (product$ or goods or item$))	17	L6
L5	L4 and 705/?.clas.	0	L5
L4	L3 and "decryption key"	56	L4
L3	L2 and memory	393	L3
L2	L1 and transaction and (encrypt$ or decrypt$ or crypto$) and @ad<=19980413	456	L2
L1	atm and bank	3000	L1

END OF SEARCH HISTORY

Your wildcard search against 10000 terms has yielded the results below.

Your result set for the last L# is incomplete.

The probable cause is use of unlimited truncation. Revise your search strategy to use limited truncation.

Generate Collection | Print

Search Results - Record(s) 1 through 10 of 30 returned.

□ 1. Document ID: US 6304169 B1

L11: Entry 1 of 30 File: USPT Oct 16, 2001

US-PAT-NO: 6304169
DOCUMENT-IDENTIFIER: US 6304169 B1

TITLE: Inductor-capacitor resonant circuits and improved methods of using same

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 2. Document ID: US 6122704 A

L11: Entry 2 of 30 File: USPT Sep 19, 2000

US-PAT-NO: 6122704
DOCUMENT-IDENTIFIER: US 6122704 A

TITLE: Integrated circuit for identifying an item via a serial port

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 3. Document ID: US 6112502 A

L11: Entry 3 of 30 File: USPT Sep 5, 2000

US-PAT-NO: 6112502
DOCUMENT-IDENTIFIER: US 6112502 A

TITLE: Restocking method for medical item dispensing system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 4. Document ID: US 6092317 A

L11: Entry 4 of 30 File: USPT Jul 25, 2000

US-PAT-NO: 6092317
DOCUMENT-IDENTIFIER: US 6092317 A

TITLE: Pop-up items having pressure-sensitive adhesive

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw. Desc | Image

□ 5. Document ID: US 6048690 A

L11: Entry 5 of 30 File: USPT Apr 11, 2000

US-PAT-NO: 6048690
DOCUMENT-IDENTIFIER: US 6048690 A

TITLE: Methods for electronic fluorescent perturbation for analysis and electronic perturbation catalysis for synthesis

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw. Desc | Image

□ 6. Document ID: US 6036101 A

L11: Entry 6 of 30 File: USPT Mar 14, 2000

US-PAT-NO: 6036101
DOCUMENT-IDENTIFIER: US 6036101 A

TITLE: Electronic labeling systems and methods and electronic card systems and methods

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw. Desc | Image

□ 7. Document ID: US 6025071 A

L11: Entry 7 of 30 File: USPT Feb 15, 2000

US-PAT-NO: 6025071
DOCUMENT-IDENTIFIER: US 6025071 A

TITLE: Removable grade hot melt pressure sensitive adhesive

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw. Desc | Image

□ 8. Document ID: US 5982284 A

L11: Entry 8 of 30 File: USPT Nov 9, 1999

US-PAT-NO: 5982284
DOCUMENT-IDENTIFIER: US 5982284 A

TITLE: Tag or label with laminated thin, flat, flexible device

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments   KWIC
Draw Desc | Image

□ 9. Document ID: US 5867265 A

L11: Entry 9 of 30   File: USPT   Feb 2, 1999

US-PAT-NO: 5867265
DOCUMENT-IDENTIFIER: US 5867265 A

TITLE: Apparatus and method for spectroscopic product recognition and identification

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments   KWIC
Draw Desc | Image

□ 10. Document ID: US 5841349 A

L11: Entry 10 of 30   File: USPT   Nov 24, 1998

US-PAT-NO: 5841349
DOCUMENT-IDENTIFIER: US 5841349 A

TITLE: Alarm tag

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments   KWIC
Draw Desc | Image

Generate Collection | Print

Terms	Documents
(attach$ with (product or goods or item) with electronic$ with (label$ or tag$ or indicia)) and @ad<=19980413	30

Display Format: TI | Change Format

Previous Page   Next Page

WEST

Your wildcard search against 10000 terms has yielded the results below.

Your result set for the last L# is incomplete.

The probable cause is use of unlimited truncation. Revise your search strategy to use limited truncation.

Generate Collection | Print

Search Results - Record(s) 11 through 20 of 30 returned.

□ 11. Document ID: US 5822194 A

```
L11: Entry 11 of 30                File: USPT                  Oct 13, 1998

US-PAT-NO: 5822194
DOCUMENT-IDENTIFIER: US 5822194 A

TITLE: Electronic part mounting device
```

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments   KWIC

Draw Desc | Image

□ 12. Document ID: US 5793305 A

```
L11: Entry 12 of 30                File: USPT                  Aug 11, 1998

US-PAT-NO: 5793305
DOCUMENT-IDENTIFIER: US 5793305 A

TITLE: Article sorting system
```

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments   KWIC

Draw Desc | Image

□ 13. Document ID: US 5778574 A

```
L11: Entry 13 of 30                File: USPT                  Jul 14, 1998

US-PAT-NO: 5778574
DOCUMENT-IDENTIFIER: US 5778574 A

TITLE: Audible product merchandising tag
```

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments   KWIC

Draw Desc | Image

□ 14. Document ID: US 5751919 A

```
L11: Entry 14 of 30                File: USPT                  May 12, 1998
```

US-PAT-NO: 5751919
DOCUMENT-IDENTIFIER: US 5751919 A

TITLE: System and method for printing overlays for electronic display devices

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 15. Document ID: US 5715555 A

L11: Entry 15 of 30 File: USPT Feb 10, 1998

US-PAT-NO: 5715555
DOCUMENT-IDENTIFIER: US 5715555 A

TITLE: Smart laundry system and methods therefor

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 16. Document ID: US 5689239 A

L11: Entry 16 of 30 File: USPT Nov 18, 1997

US-PAT-NO: 5689239
DOCUMENT-IDENTIFIER: US 5689239 A

TITLE: Identification and telemetry system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 17. Document ID: US 5687495 A

L11: Entry 17 of 30 File: USPT Nov 18, 1997

US-PAT-NO: 5687495
DOCUMENT-IDENTIFIER: US 5687495 A

TITLE: Pop-up items having pressure-sensitive adhesive

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 18. Document ID: US 5523749 A

L11: Entry 18 of 30 File: USPT Jun 4, 1996

US-PAT-NO: 5523749
DOCUMENT-IDENTIFIER: US 5523749 A

TITLE: Identification system for simultaneously interrogated labels

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments KWIC

Draw. Desc | Image

□ 19. Document ID: US 5510769 A

L11: Entry 19 of 30 File: USPT Apr 23, 1996

US-PAT-NO: 5510769
DOCUMENT-IDENTIFIER: US 5510769 A

TITLE: Multiple frequency tag

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments KWIC

Draw. Desc | Image

□ 20. Document ID: US 5444223 A

L11: Entry 20 of 30 File: USPT Aug 22, 1995

US-PAT-NO: 5444223
DOCUMENT-IDENTIFIER: US 5444223 A

TITLE: Radio frequency identification tag and method

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments KWIC

Draw. Desc | Image

Generate Collection | Print

Terms	Documents
(attach$ with (product or goods or item) with electronic$ with (label$ or tag$ or indicia)) and @ad<=19980413	30

Display Format: TI | Change Format

Previous Page Next Page

WEST

Your wildcard search against 10000 terms has yielded the results below.

Your result set for the last L# is incomplete.

The probable cause is use of unlimited truncation. Revise your search strategy to use limited truncation.

Generate Collection | Print

Search Results - Record(s) 21 through 30 of 30 returned.

□ 21. Document ID: US 5315096 A

```
L11: Entry 21 of 30                File: USPT                    May 24, 1994

US-PAT-NO: 5315096
DOCUMENT-IDENTIFIER: US 5315096 A

TITLE: Deactivator for resonance labels
```

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 22. Document ID: US 5218189 A

```
L11: Entry 22 of 30                File: USPT                    Jun 8, 1993

US-PAT-NO: 5218189
DOCUMENT-IDENTIFIER: US 5218189 A

TITLE: Binary encoded multiple frequency RF indentification tag
```

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 23. Document ID: US 5198650 A

```
L11: Entry 23 of 30                File: USPT                    Mar 30, 1993

US-PAT-NO: 5198650
DOCUMENT-IDENTIFIER: US 5198650 A

TITLE: Hands free/hand held bar code scanner
```

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 24. Document ID: US 5151684 A

```
L11: Entry 24 of 30                File: USPT                    Sep 29, 1992
```

US-PAT-NO: 5151684
DOCUMENT-IDENTIFIER: US 5151684 A

TITLE: Electronic inventory label and security apparatus

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 25. Document ID: US 4920335 A

L11: Entry 25 of 30 File: USPT Apr 24, 1990

US-PAT-NO: 4920335
DOCUMENT-IDENTIFIER: US 4920335 A

TITLE: Electronic article surveillance device with remote deactivation

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 26. Document ID: US 4833609 A

L11: Entry 26 of 30 File: USPT May 23, 1989

US-PAT-NO: 4833609
DOCUMENT-IDENTIFIER: US 4833609 A

TITLE: ERC with operator prompting for entering quantity of selected multi-item packaged goods

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 27. Document ID: US 4535557 A

L11: Entry 27 of 30 File: USPT Aug 20, 1985

US-PAT-NO: 4535557
DOCUMENT-IDENTIFIER: US 4535557 A

TITLE: Label for the identification of objects and apparatus for using said label

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

□ 28. Document ID: US 4257669 A

L11: Entry 28 of 30 File: USPT Mar 24, 1981

US-PAT-NO: 4257669
DOCUMENT-IDENTIFIER: US 4257669 A

TITLE: Optical-electronic system for the identification of a retro-reflective label

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments   KWIC
Draw Desc | Image

□ 29. Document ID: US 4158434 A

L11: Entry 29 of 30   File: USPT   Jun 19, 1979

US-PAT-NO: 4158434
DOCUMENT-IDENTIFIER: US 4158434 A

TITLE: Electronic status determining system for goods

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments   KWIC
Draw Desc | Image

□ 30. Document ID: US 3707711 A

L11: Entry 30 of 30   File: USPT   Dec 26, 1972

US-PAT-NO: 3707711
DOCUMENT-IDENTIFIER: US 3707711 A

TITLE: ELECTRONIC SURVEILLANCE SYSTEM

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments   KWIC
Draw Desc | Image

Generate Collection | Print

Terms	Documents
(attach$ with (product or goods or item) with electronic$ with (label$ or tag$ or indicia)) and @ad<=19980413	30

Display Format: TI | Change Format

Previous Page   Next Page

WEST

Generate Collection | Print

Search Results - Record(s) 1 through 3 of 3 returned.

□ 1. Document ID: US 6442276 B1

```
L10: Entry 1 of 3                File: USPT                Aug 27, 2002

US-PAT-NO: 6442276
DOCUMENT-IDENTIFIER: US 6442276 B1

TITLE: Verification of authenticity of goods by use of random numbers
```

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw Desc | Image

---

□ 2. Document ID: US 5745573 A

```
L10: Entry 2 of 3                File: USPT                Apr 28, 1998

US-PAT-NO: 5745573
DOCUMENT-IDENTIFIER: US 5745573 A

TITLE: System and method for controlling access to a user secret
```

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw Desc | Image

---

□ 3. Document ID: US 5557765 A

```
L10: Entry 3 of 3                File: USPT                Sep 17, 1996

US-PAT-NO: 5557765
DOCUMENT-IDENTIFIER: US 5557765 A

TITLE: System and method for data recovery
```

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw Desc | Image

---

Generate Collection | Print

Terms	Documents
L9 and (product$ with authentic$)	3

WEST

□ Generate Collection Print

L10: Entry 1 of 3 File: USPT Aug 27, 2002

DOCUMENT-IDENTIFIER: US 6442276 B1
TITLE: Verification of authenticity of goods by use of random numbers

DATE FILED (1):
19970721

Abstract Text (1):

A method of verifying the authenticity of goods includes generating one or more random codes and storing the one or more random codes in a database. The goods are then marked with one of the generated random codes such that each of the goods contain their own unique random code. Upon field checking and inventory of marked goods and comparing the codes on the marked goods to codes within the database, the authenticity of goods may be verified. Also, a system for verifying the authenticity of goods includes a database containing a plurality of unique random codes and an indication whether each of the unique random codes has been read, and a code reader or scanner for reading the code affixed to a good. The system further includes a computer apparatus or other electrical mechanism for comparing a read code to the unique random codes contained within the database such that upon comparison the comparing means indicates whether the read code is valid and if valid, whether it has been read previously on another good, thereby indicating the good's authenticity.

Brief Summary Text (4):
Products which are mass produced are distributed to end users through sales and distribution channels. When the products have particular value associated with them, counterfeiters sometimes produce products which are copies of those produced by the original manufacturers. These counterfeit products are then introduced into the sales and distribution channels and end users become deceived regarding the source of the goods and/or their quality. Lost sales occur for the original manufacturer, and the end user may receive less value than what was expected. Name brand goods, certified products and copyrighted products are often the target of such counterfeiting activities.

Brief Summary Text (5):
To address the problem of counterfeiting, one prior art solution has been to attach a label containing an optical device which is difficult to reproduce, for example, a holographic image to the products to confirm their authenticity. The original manufacturer controls these labels and their content to prevent easy access to such labels by counterfeiters. Use of such an optical device is desirable in that the authentication procedure is relatively simple, for anyone may visually inspect the label and its presence indicates authenticity. Unfortunately, this approach suffers from the weakness that skilled counterfeiters, by extending substantial effort, can reproduce these labels. Once reproduction is achieved, the counterfeiter may easily introduce a multitude of counterfeit products within the sales and distribution channels. A second disadvantage to the optical device methodology is that the creation of the special labels is relatively expensive and therefore is only cost effective for certain classes of products.

Brief Summary Text (6):
In pre-paid service areas, the use of randomly generated numbers have been utilized to validate a user prior to accessing the pre-paid service. For example, pre-paid phone card access numbers generated by random numbers have been used for such purposes. The phone card number is input into a phone or other device to validate the user prior to registering a phone call. A second application involves the use of confirmation numbers as back-up identification for electronic ticketing air fares.

The use of random numbers for access of such pre-paid services, however, is substantially different than the use of optical codes for authenticating mass produced goods. For example, in the pre-paid phone card application, each random number is held secret by the user of the service, therefore a theft of the phone card or its loss may allow someone to access the pre-paid service. In the electronic air fare ticketing application, neither secrecy nor duplication of the code is of great concern since the use of the random number is only for backup identification. Knowledge of the confirmation number by a third party is unlikely to cause any loss because a third party's attempt to board an airplane flight will conflict with the boarding by the valid party. Unlike the product authentication in which previously optical devices have been used, the pre-paid service using randomly generated numbers play no role in preventing or deterring large scale loss due to counterfeiting of mass-produced goods.

Brief Summary Text (7):
In another prior art method for authentication, an apparatus is used to measure a random characteristic of a card, tag or label. The random characteristic, or "fingerprint," is read by a special reading apparatus and converted to a code which is encrypted and printed on the tag or label. The encryption ties the label to the original manufacturer of the product and the code value in turn is tied to the particular label on which it is printed since that label has the "fingerprint." This method, although secure in authenticating single labels, introduces significant costs because the label must contain special technology for the development of the "fingerprint" and a special reader must be developed and used at the time of printing the label and when the label is subsequently field checked. These shortcomings introduce significant costs in attempting to authenticate mass produced goods. It is not necessary to prevent even single counterfeits, which this method does, since the manufacturer of mass produced goods is instead interested in deterring mass counterfeiting of his product.

Brief Summary Text (11):
In another aspect of the invention, a system for verifying the authenticity of goods includes a database containing a plurality of unique random codes and an indication whether each of the unique random codes has been read, and a code reader or scanner for reading the code affixed to a good. This system further includes a comparing means for comparing a read code to the unique random codes contained within the database such that upon comparison the comparing means indicates whether the read code is valid and if valid, whether it has been read previously on another good, thereby indicating the good's authenticity.

Brief Summary Text (12):
The verification system further includes a computer for generating the plurality of unique random codes which includes a memory for containing each of the generated random codes. The computer, upon generating a random code, compares the code to a list of previously generated codes within the memory and eliminates any generated code that is a duplicate, thereby ensuring that each generated code is unique. The verification system also includes a printer, in electrical communication with the computer, for printing the generated random codes on a tag, label or directly upon the good to be marked. The printer is capable of printing either the generated code alone, or each generated code with its corresponding bar code equivalent to the tag, label or directly on the product to aid in the subsequent reading of the code. The system may further include a scanner for reading the printed codes.

Brief Summary Text (13):
In another aspect of the invention, a method of detecting diversion of goods from a desired channel or channels of distribution includes the generation of an encrypted code, wherein the code has a random portion and a non-random portion. The encryption of this code is effectuated by an encryption key wherein each encryption key is unique to a desired channel or channels of distribution. The encrypted codes are applied to goods such that each good has its own unique encrypted code. Subsequently, within the desired channel or channels of distribution, the various goods are inspected and it is verified whether the decryption key used on the code successfully reproduces the non-random portion which is uniquely dedicated for the desired channel or channels of distribution. Consequently, the method identifies whether a diversion of goods has occurred if the decryption key does not match that used on the inspected goods.

Detailed Description Text (2):
The system and method of the following invention provides for the verification of

authenticity of goods [illegible] use of random numbers. Random numbers, codes or encrypted combination codes including a random code and a non-random code are generated by a computer and subsequently produced on tags, labels or directly on products and ultimately placed within the stream of commerce. At a retail distribution outlet such as a retail store or alternatively, at any point earlier in the distribution chain, the codes are read from the marked products and compared to random codes contained within a database in which the codes are stored upon their initial generation. If the scanned product code is not verified as a valid code, the product is identified as a counterfeit. If the product code is a valid product code a further inquiry may be made to determine whether the valid code has previously been used. If the code has previously been used, the product is identified as a counterfeit; if not, an indication is made within the database that the valid code has now been used. Alternatively, the encrypted combination codes are decrypted and read to identify its non-random portion. If the decrypted non-random portion matches the originally used non-random code, goods are authenticated while a mismatch indicates a counterfeit. The present system and method allows for a cost-effective verification of authenticity of goods and provides a substantial deterrent to those who wish to counterfeit mass produced items.

Detailed Description Text (3):
FIG. 1 is a combined system and method diagram which illustrates the various components of the present invention and provides an environmental context in which the various components are utilized; FIG. 1 therefore illustrates an authentication system 10. The authentication system 10 includes a host computer 12 having a processor 14 which contains the requisite hardware and software to provide a random number generator 16 and an encryptor 18. The processor 14 is coupled to an internal memory 20 for storage of generated random numbers or codes or alternatively for storage of various encryption algorithms to ensure that each code or encryption technique is unique. The processor 14 is also coupled to an I/O module 22 which provides input and output circuitry, drivers and interfaces to communicate with external components such as keyboards, printers and other peripherals or networks. Although the memory 20 has been illustrated as an internal memory, it should also be understood that the host computer 12 may alternatively utilize and access external memory. Upon generation of each random code, the processor 12 stores the random codes in a secure host database 24 for later access by field checkers to verify product authenticity.

Detailed Description Text (4):
The host computer 12 is coupled to a printer 26 via the I/O module 22. The printer 26 receives random codes generated by the processor 14 within the host computer 12 via the I/O module 22 and is operable to print out the random codes on various print media, for example, tags, labels or directly on various products. Depending upon the type of random code or combination code created by the random code generator 16, the printer 26 may generate a binary code 28 having a corresponding bar code for ease of reading or scanning, an alphanumeric code 30 having a corresponding bar code or alternatively a case sensitive alphanumeric code 32 with its corresponding bar code. Alternatively, other type codes may also be used. Depending upon the type of product being marked, the printer 26 generates the codes on a tag or label 34 (or alternatively directly on a product) which is then attached or affixed to the products 36, which are exemplary illustrated as the plurality of pants (clothing) which constitute a product inventory 38. Each product 36 is therefore marked with the label or tag 34, wherein each product 36 contains a unique random or combination code generated within the host computer 12. The products 36 are then distributed in commerce via various modes of transportation 40, for example, by air 42, by rail 44 or by standard freight shipping 46 to ultimately arrive at a retail distributor (or outlet) 48.

Detailed Description Text (5):
At the retail outlet 48 the label or tag 34 affixed to the product 36 is read by a tag reader (or scanner) 50 which is electrically coupled to the retail outlet's local computer 52. The local retail computer 52 is also in electrical communication with the secure host database 24 via a network-type connection 54. Various methods may be implemented utilizing the authentication system of FIG. 1; for example, the system 10 may not only verify the authenticity of mass produced products, but may also be used to identify a diversion of such products into undesired channels of distribution.

Detailed Description Text (6):
Turning now to FIG. 2, a method for verifying the authenticity of mass produced

products via use of random codes utilizing the authentication system 10 of FIG. 1 will be described. At step 60, the authentication system 10 generates one or more random codes. The one or more random codes are preferably generated within the host computer 12 via a user requesting such generation via an input device such as a keyboard which is coupled to the I/O module 22 which, in turn, is coupled to the processor 14. Upon such request, the processor 14 initiates generation of such a code via the random number (code) generator 16. Upon generation, the processor 14 checks whether the generated random code has been previously generated by comparing the generated random code to previously generated codes resident within the memory 20. If the generated random code has previously been generated, the processor 14 will erase the random code and generate another. The processor 14 may look within the memory 20 for all previous products made, or alternatively, or look within various subdirectories within the memory 20 to see whether the generated random code has been previously generated for the specified product now being addressed. Otherwise, the generated code is determined to be unique. The generation of random numbers in software is well known by those skilled in the art. For example, see "Suggestions for Random Number Generation in Software" by Tim Matthews, An RSA Data Security Engineering Report, Revised Dec. 26, 1995, which is hereby incorporated by reference in its entirety.

Detailed Description Text (8):
Upon the completion of product marking, the marked products are placed into the flow of commerce at step 66 via any of the modes of transportation 40 which are highlighted in FIG. 1. Generally, such transportation constitutes standard freight shipping 46 such as by truck. The marked products 36 are then delivered to the retail outlet 48 where the marked products are read by a reading device or scanner 50 at step 68. Preferably, the label 34 on the product 36 is scanned by the scanner 50 upon the product's initial arrival at the retail outlet 48. Alternatively, the scanning may also be completed at a later time, for example, when the article is being purchased by a consumer. The scanner 50 scans the code on the tag 34, preferably by scanning the bar code which is a visual representation of the binary or alphanumeric random code being utilized. The scanner 50 takes the random code that has been scanned and downloads the scanned random code to the local computer 52.

Detailed Description Text (9):
The local computer 52 may be utilized for various accounting and inventory purposes in addition to the verification of authenticity of goods. In addition, the local computer 52 is in electrical communication with the secure host database 24 via either a wireless or wired network 54 or communication data link. The local computer 52, in accessing the secure host database 34, then compares the scanned random product code to those codes contained within the secure host database 24 at step 70 to verify whether the scanned random code is valid at step 72. If the scanned product code is not contained within the database 24 then the local computer 52 indicates to the individual performing the scan that the article is a counterfeit. Conversely, if the scanned product code is valid, that is, it has been found in the secure host database 24, the local computer 52 then checks the database 24 to see whether the scanned code has previously been used at step 74. If the database 24 indicates that the code has previously been used, the local computer 52 indicates to the user that the code is a duplicate. In this instance, one of two possibilities exist: either the present goods scanned are a counterfeit, or the product is authentic and the previously used code was attached to a counterfeit article. In either case, evidence of illegal counterfeiting activity has been uncovered. If the local computer 52, after analyzing the database 24, determines that the code has not previously been used, it indicates to the user that the goods are authentic and additionally indicates within the database 24 that a valid code has now been used at step 76. In this manner, the above method verifies the authenticity of mass produced products through use of random codes placed on the articles which are subsequently checked against a secure database whether the articles are at their retail outlet or perhaps at an intermediary wholesale location.

Detailed Description Text (10):
The effectiveness of the above-described method may be more fully appreciated through the following discussion of the method of FIG. 2. Suppose, for example, the type of random code chosen is a 64 bit binary code. The number of possible 64 bit binary codes is 2.sup.64, which is 1.8.times.10.sup.19 different numbers. Further suppose that a manufacturer wishes to mark 100 million similar products to verify their authenticity. 100 million unique 64 bit codes are then randomly chosen, stored in the secure database 24, and then each unique random code is applied to each

respective product in a form which is preferably removal resistant and perhaps even tamper-evident. Because this application of a product marking to the product itself is normally done, no significant incremental cost is associated with this operation. Further, since 100 million mass produced products have been marked and 1.8.times.10.sup.19 different codes are available, the probability of a counterfeiter guessing one of the used random codes is only 1 in 1.8.times.10.sup.11. Therefore it is virtually impossible for a counterfeiter to come up with a significant number of valid codes without extending a considerable amount of effort and expense. For example, a counterfeiter must go to various retail outlets 48 and copy a number of valid random codes. This is an expensive and laborious process and further subjects the counterfeiter to potential discovery in the copying process. Additionally, whenever a counterfeiter applies a code which has been copied from products out in the field to his counterfeit products, the counterfeiter ends up labeling the product with a duplicate code. As already shown, all duplicates in the above method will be discovered which allows for subsequent investigation as to the source of the counterfeit product to identify the counterfeiter.

Detailed Description Text (13):
In the embodiment discussed with respect to FIG. 2, the authentication system 10 utilizes field checking and subsequent validation and verification of codes between the local computer 52 and the secure host database 24 via the network data link 54. Therefore in that discussion, it is evident that the database 24 interacts with the local computer 52 to the extent that codes which have been read in previous field checking are labeled as such and identified with the sales outlet in which they are found. So, when accessed from the retail outlet 48, the database 24 updates this information in addition to determining that the valid code is present in the database and is not a duplicate. In this manner, verification of product authenticity is made at the time of database access. However, this is not the only solution. Alternatively, such verification may be accomplished locally at the retail outlet 48 field check location without access to a secure master database.

Detailed Description Text (14):
Proceeding on to FIG. 3, a method of verifying the authenticity of products without accessing an off-site master database will be described in conjunction with the authentication system 10 of FIG. 1. At step 80, the generation of random codes is established in a manner similar to that described earlier in step 60 of FIG. 2; consequently, the details of such random code generation will not be repeated. At step 81, each random code is combined with a non-random code to thereby form a combination code. The non-random code may be, for example, the initials of the manufacturer, a tradename or other easily recognizable moniker or message, and combining may simply be accomplished by concatenating the initials to the end of each random code. Alternatively, the non-random code may be placed before or even interposed within the random code. Subsequent the generation of this combination code, the combination codes are encrypted at step 82 by the processor 14 within the host computer 12 which accomplishes the encryption via an internal encryptor 18. The encryptor 18, in a preferred embodiment, is a combination of processor hardware and software which allows for encryption of the generated combination codes which are developed from the random number generator 16 by concatenating each of its outputs with the non-random code. Preferably, the encryptor 18 uses an encryption key that is unique to each product manufacturer such that each manufacturer's products have their own unique encryption scheme. Preferably, the encryptor 18 uses an encryption scheme known as a public key cryptosystem. Such cryptosystems use two related keys, one for encryption and the other for decryption. One is kept private and the other is made public. After encryption, both the generated combination code (random number and its non-random portion) and its encrypted counterpart are both saved within the memory 20 for later comparison with subsequently generated random numbers to ensure that each generated random number and its encrypted counterpart are unique. After encryption, the encrypted combination code is generated via communication between the I/O module 22 and the printer 26. The printer 26 prints each encrypted combination code on a single tag so that each tag contains an encrypted combination code as well as its bar code representation. Therefore the code on each tag will consist of only an encrypted counterpart since the constant portion of the combination code is known. Again, as discussed earlier, these codes may be either a binary code 28, an alphanumeric code 30, a case sensitive alphanumeric code 32 as illustrated in FIG. 1 or any other type code.

Detailed Description Text (15):
At step 84, the tags containing the encrypted combination codes are placed on

products such that each product contains its own unique encrypted combination code and each product is then placed in the stream of commerce at step 86. Upon reaching the retail distributer or outlet 48 the encrypted combination code is read at step 88 before the various products 36 are accessible to the regular consumers. The scanner 50 scans the encrypted combination code at step 88 and downloads it to the local computer 52 which contains a decryption key which is unique and provided by the manufacturer (the public key). The local computer 52 then decrypts the read encrypted code at step 90 and compares the decrypted code to the already known non-random code portion at step 92.

Detailed Description Text (16):
At step 94 the local computer 52 checks to see whether the already known non-random code portion and the decrypted code that had been read by the scanner 50 match. If the decrypted code and the non-random code portion do not match, the local computer provides an indication to the checker by either an audible or visual indicator that the product 36 is a counterfeit. The manner in which one recognizes the non-random portion of the combination code may be more easily understood in conjunction with FIG. 4. FIG. 4 is a chart 99 in which eight different encrypted combination codes have each been decrypted using a public encryption key. Note that each decrypted combination code has the same non-random code portion "YOU" at the end. Consequently, a checker can easily verify the authenticity since they know what the non-random code portion should be although the checker will not know the intricacies of the public key decryption methodology. As stated earlier, the non-random portion of the combination code may be a tradename, the manufacturer's initials, or any type of recognizable message. Alternatively, the local computer 52, after decryption, may display the decrypted code on a display portion of the scanner 50 so that the user scanning the tags can visually view the non-random code portion and thereby verify authenticity.

Detailed Description Text (17):
If a match is found, the local computer 52 checks to see whether this code has previously been scanned by the scanner 50 at step 96 by analyzing the random portion of the code which is unique for each combination code. If this code has previously been used at that locality, then the local computer 52 provides an indication that the product 36 is a counterfeit at step 96. Alternatively, a master database containing used codes may also be maintained in which various local computers 52 at various retail outlets 48 are connected together to indicate the identification of various valid codes so that the verification of whether a code has been used in step 96 may be even more extensive. Finally, at step 98, if the identified valid code has not been used the local computer 52 provides an indication to the user that the code is valid and therefore the goods are authentic and further provides an indication either within its own memory or within the master database that the code has been used for any subsequent checking.

Detailed Description Text (18):
In the above-described method of FIG. 3, a counterfeiter has few alternatives to try to defeat this method. The counterfeiter must create its own encryption method or encryption keys which will not match the encryption method or keys utilized to generate the encrypted combination codes in step 82 and therefore the decryption of the encrypted combination code will not match the already known non-random portion of the combination code in step 94 and a counterfeit will be detected. Further, if the counterfeiter chooses to copy codes after they become accessible to the public, these duplicate codes can be detected at step 96 since use of duplicate codes will be identified. Note also that a theft of the field checker's local computer 52 will not compromise the security provided by the host computer 12 since the local computer 52 contains a decryption key and a database listing of used codes. Recall that in a public key cryptosystem knowing the decryption key gives no knowledge of the encryption key. None of this information, therefore, is advantageous to the counterfeiter because it does not provide information regarding how to encrypt the codes nor does it indicate the existence of valid, presently unused codes.

Detailed Description Text (19):
The combination codes of FIGS. 3 and 4 provide an additional level of security by thwarting a counterfeiter who intercepts the field verifier (public key) and replaces them with his own verifier. If a counterfeiter steals the verifier and replaces it with one that includes the legitimate public key (obtained by analyzing the intercepted devices) and an additional bogus public key with control software, the counterfeiter will be able to inject counterfeit goods into the market that will appear valid via an analysis of the decrypted non-random code portion. However, as

discussed earlier, the random code portions can be made virtually unguessable and the decrypted random code portions can be compared to a secure master database to see if the code is a valid random code that has not previously been used. Consequently, the combination provides another level of additional security, if desired.

Detailed Description Text (20):
Another alternative embodiment of the present invention relates to a method and system for identifying an undesired diversion of goods from a desired channel or channels of distribution and is illustrated in FIG. 5. The manner in which the method is performed will be discussed in conjunction with various components of the authentication system 10 of FIG. 1. At step 100, a pair of encryption keys (wherein the first, the private key, encrypts a code and the second, the public key, decrypts the encrypted code) are generated by the host computer 12. The encryptor 18 within the processor 16 generates the encryption key pairs, one key pair for each distribution channel through which the manufacturer intends to ship his goods.

Detailed Description Text (21):
After a unique pair of encryption keys are generated by the computer 12 at step 100, and wherein this unique pair of keys is associated with a particular channel of distribution through which goods are to be tracked, the private key is provided to the manufacturer of the goods at step 102 and used by the manufacturer to generate encrypted combination codes (step 104) as discussed earlier for application to the goods at step 106. The encrypted combination codes may be generated by a printer such as the printer 26 of FIG. 1 which is in electrical communication with a computer which dictates the combination code via the private encryption key. As discussed supra, the printer may apply the codes directly to the goods or alternatively may generate the codes on tags or labels for subsequent affixation to the goods. After the goods are properly marked, the goods are placed into commerce at step 108 into the particular channel of distribution via various modes of transportation (see, for example, FIG. 1, reference numerals 42, 44 and/or 46).

Detailed Description Text (22):
To determine whether a diversion of the goods into an undesired channel of distribution has occurred, an inspection of the goods within the expected channel of distribution is undertaken by the manufacturer at step 110. Inspection of the goods involves scanning the encrypted combination codes with a scanner 50 which is in electrical communication with a local computer such as computer 52 of FIG. 1 which contains the public encryption key which is associated with a particular distribution channel. At step 112, a determination is made whether or not the goods have been diverted by decrypting the encrypted combination code with the public encryption (decryption) key. If the decrypted code matches the already known non-random portion of the combination code no diversion has occurred, however, if no match is obtained, a diversion of goods from the desired channel of distribution has been discovered. Upon discovery, the manufacturer may then retrace the product shipments to identify the source of the diversion. To this end the manufacturer may use other public keys which are associated with other distribution channels to decrypt the encrypted combination code until he finds a match. In this way he can find the distribution channel into which the goods were first shipped.

Detailed Description Text (23):
Various modifications may be made to the above system and methods which also fall within the scope of this invention. For example, instead of utilizing an encryption technique on the combination codes, a digital signature of the random code may be generated by use of a one-way hash function and, in conjunction with a private key, used to calculate an encrypted number. This encrypted number along with the random number code forms a two-part code which is placed on the product. The manufacturer may now inspect this two-part code by decrypting the encrypted number with the public key to obtain the number. This number may then be compared with the number obtained by use of the one-way hash function with the random number code . If the numbers match, then the inspected product is determined to be authentic.

Detailed Description Text (24):
Another alternative is to place the random code or the encrypted combination code on the product in a location that is hidden from view such that the reading of the code can only occur by tampering with the product in an irreversible manner such that the code is tamper evident. A simple example is illustrated in FIG. 6, wherein a code 150 is affixed to an inside cover 151 of a sealed package 152. A seal 153 on the package 152 must be broken and the cover opened in order to read the code 150.

Further, such reading may lower or destroy the value of the product whose code is being read. In this manner, a counterfeiter who attempts to gather valid codes from the goods within the distribution channel has an expensive task since great economic expense is incurred when attempting to copy a meaningfully large number of valid codes. Further, a manufacturer's need to check codes on products within the distribution channel in order to statistically determine a lack of duplicity is dramatically reduced. A counterfeiter will gather fewer codes as a result of the above-described added expense and it follows that his goods will have a proportionately higher number of duplicates. More duplicates makes any sampling program operated by the manufacturer more likely to find duplicates. Therefore, the manufacturer may choose to reduce his sampling program to save costs and still maintain high likelihood of discovering duplicates.

Detailed Description Text (25):
Yet another alternative embodiment is to create a two-part code such as that described in connection with the digital signature embodiment and apply the random number code overtly to the product and apply the encrypted number code covertly to the product. For example, as illustrated in FIG. 7, an encrypted code 160 may be placed on a package 162. The second code portion 164 is covert such that it is not easily detectable. Various covert type codes are contemplated. In this example, an invisible ink code is utilized which may be detected when irradiated with ultra-violet light from a UV source 166. Various other covert type coding techniques, however, are contemplated by the present invention. In another example, the encrypted code may be placed inside the package so that it is both time consuming and/or destructive (or defacing) to the product when attempting to observe it. In this manner, checking for whether the random code is a duplicate is easy since only the external code need be examined. Then, in order to check whether the goods are genuine, the manufacturer can sample a small percentage of the product. This technique makes it costly to gather a significant number of valid code pairs to mask counterfeiting activity.

Detailed Description Text (26):
The present invention is contemplated in the context of various types of mass produced goods. Although the above examples highlighted the invention in the context of consumer goods such as clothing apparel, etc. the invention is also applicable to other type goods. For example, the present invention may be incorporated with computer software in which the coding is placed on the packaging itself or alternatively may be placed on the storage media itself such as optical media in CD-ROMs or magnetic media such as diskettes, etc. In this context the scanner is replaced by the magnetic or optical head that reads the information on the disk and performs the encryption, etc. as highlighted above.

CLAIMS:

4. The method of claim 1, wherein the step of inspecting the inventory of marked goods comprises reading the one or more encrypted combination codes with a scanner.

17. The system of claim 12, wherein the code reader is a scanner.

20. The method of claim 18, wherein the step of verifying further comprises: inspecting the goods within the desired channel or channels of distribution; decrypting the codes on the goods with a decryption key; and examining the decrypted codes, thereby determining whether a diversion of goods has occurred.

22. The method of claim 20, wherein the step of inspecting the goods comprises reading the codes on the goods with a scanner.

24. The method of claim 18, further comprising the step generating a pair of encryption keys, wherein one key is used to encrypt combination codes and the other is used to decrypt the codes within the desired channel or channels of distribution.

26. The method of claim 24, further comprising if an encrypted combination code cannot be decrypted by an encryption key used to decrypt the codes within the desired channel or channels of distribution, attempt decryption of the encrypted combination code by an encryption key used to decrypt the codes within a different channel or channels of distribution to search for the distribution channel into which the goods were earlier shipped.

29. The method of claim 18, wherein the error in distribution is a diversion of goods, wherein the combination codes are encrypted using a private encryption key, and the verifying comprises using a public decryption key for the desired channel or channels of distribution, and wherein if the desired channel or channels of distribution cannot be verified using the public decryption key, then further comprising using a further public decryption key designated for a different channel or channels of distribution to discover the incorrect channel or channels of distribution.

39. The method of claim 38, wherein the step of reading the code comprises scanning the code.

67. The method of claim 61, wherein the combination codes are encrypted by a private key, and said inspecting comprises using a public key to decrypt the encrypted combination codes.

□	4868877	September 1989	Fischer	380/25
□	4926480	May 1990	Chaum	380/30
□	4947430	August 1990	Chaum	380/25
□	4996711	February 1991	Chaum	380/30
□	5005200	April 1991	Fischer	380/30
□	5144665	September 1992	Takaragi et al.	380/30
□	5191611	March 1993	Lang	380/25
□	5200999	April 1993	Matyas et al.	380/30
□	5210795	May 1993	Lipner et al.	380/23
□	5214702	May 1993	Fischer	380/30
□	5224163	June 1993	Gasser et al.	380/25
□	5226080	July 1993	Cole et al.	380/25
□	5263157	November 1993	Janis	380/4
□	5265163	November 1993	Golding et al.	380/25
□	5265164	November 1993	Matyas et al.	380/30
□	5267313	November 1993	Hirata	380/21
□	5276736	January 1994	Chaum	380/25
□	5276737	January 1994	Micali	380/30
□	5276901	January 1994	Howell et al.	
□	5280527	January 1994	Gullman et al.	380/23
□	5299263	March 1994	Beller et al.	380/30
□	5313637	May 1994	Rose	380/4
□	5315658	May 1994	Micali	380/30
□	5341426	August 1994	Barney et al.	380/30
□	5347578	September 1994	Duxbury	380/4
□	5351293	September 1994	Michener et al.	380/21
□	5371794	December 1994	Diffie et al.	380/21
□	5373559	December 1994	Kaufman et al.	380/30
□	5386470	January 1995	Carter et al.	380/23
□	5406628	April 1995	Beller et al.	380/21
□	5436972	July 1995	Fischer	380/25
□	5481613	January 1996	Ford et al.	380/30
□	5557346	September 1996	Lipner et al.	380/21
□	5557765	September 1996	Lipner et al.	380/21

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0 493232	July 1992	EP	
WO92/09161	November 1991	WO	
WO 93/21708	October 1993	WO	

OTHER PUBLICATIONS

Novell, "Encryption Alternatives," comments submitted in Key Escrow Alternatives Workshop, Jun. 10, 1994.
Computer Associates International, Inc., "Commercial Cryptography Perspectives," comments submitted in Key Escrow Alternatives Workshop, Jun. 10, 1994.
Puhl, Larry, Motorola, comments submitted in Key Escrow Alternatives Workshop, Jun. 10, 1994.
Ferguson, Bill, Semaphore, comments submitted in Key Escrow Alternatives Workshop, Jun. 10, 1994.
COMPAQ Computer Corporation, "Proposed NIST Draft," comments submitted in Key Escrow Alternatives Workshop, Jun. 10, 1994.
Housley, Russell, SPYRUS, letter to Lynn McNulty, Aug. 3, 1994.
Desmedt, Yvo et al., "A Scientific Statement on the Clipper Chip Technology and Alternatives," University of Wisconsin, Milwaukee.
Maher, David p., "Trust in the New Information Age," AT&T Technical Jornal, Sep./Oct. 1994, vol. 73, No. 5, Security Technologies, pp. 9-16.
Micali, S., "Fair Cryptosystems," Aug. 11, 1993.
Bandstad et al., "Draft Proposed Escrowed Encryption Standard," viewgraphs presented at Computer Security and Privacy meeting, Mar. 1994.
Blaze, M., "Protocol Failure in the Escrowed Encryption Standard," presented on the Internet, Jun. 3, 1994.
Scheidt et al., "Private Escrow Key Management," Key Escrow Encryption Workshop, paper distributed Jun. 10, 1994.
"A Solution for the International Community," TECSEC, Key Escrow Encryption Workshop, viewgraphs distributed Jun. 10, 1994.
"Private Escrow Key Management," TECSEC, Key Escrow Encryption Workshop, viewgraphs distributed Jun. 10, 1994.
"An Advanced Key Management System," TECSEC, Key Escrow Encryption Workshop, paper distributed Jun. 10, 1994.
Denning et al., "Key Escrowing Today," IEEE Communications, Sep. 1994.
Harn, L. and H. Y. Lin, "Integration of User Authentication and Access Control," IEEE Proceedings-E, vol. 139, No. 2, pp. 139-143, Mar. 1992.
Brickell et al., "SKIPJACK Review: Interim Report: The SKIPJACK Algorithm," Georgetown University, Office of Public Affairs, pp. 1-6, Jul. 28, 1993.
Denning et al., "A Taxonomy for Key Encryption System," draft distributed Sep. 24, 1994.
Denning, D., "Key Escrow Encryption: Does it Protect of Compromise User Interest?," Jan. 3, 1995.
Denning, D., "Observations about Key Escrow Alternatives," Jan. 2, 1995.
Droge, John C., "International Key Escrow," presented to NIPLI, Sep. 22, 1994.
Ford et al., "A Key Distribution Method for Object-Based Protection," presented at the Second ACM Conference on Computer and Communications Security, Nov. 2-4, 1994, Faifax, VA., pp. 193-197.
Denning, Dorothy, "International Key Escrow Encryption: Proposed Objectives," Georgetown University, draft of May 23, 1994.
Eldridge, Alan, Lotus Notes, "Key Escrow for Lotus Notes," comments submitted in Key Escrow Alternatives Workshop, Jun. 10, 1994.
Fischer, Addison, Fischer International, "Software Key Escrow--Corporate Implementation," comments submitted in Key Escrow Alternatives Workshop, Jun. 10, 1994.

ART-UNIT: 222

PRIMARY-EXAMINER: Cangialosi; Salvatore

ABSTRACT:

A system and method for data escrow cryptography are described. An encrypting user encrypts a message using a secret storage key (KS) and attaches a data recovery field (DRF), including an access rule index (ARI) and KS, to the encrypted message. The DRF and the encrypted message are stored in a storage device. To recover KS, a

decrypting user extracts and sends the DRF to a data recovery center (DRC) that issues a challenge based on access rules (ARs) originally defined by the encrypting user. If the decrypting user meets the challenge, the DRC sends KS in a message to the decrypting user. Generally, KS need not be an encryption key but could represent any piece of confidential information that can fit inside the DRF. In all cases, the DRC limits access to decrypting users who can meet the challenge defined in either the ARs defined by the encrypting user or the ARs defined for override access.

35 Claims, 31 Drawing figures

WEST

□ Generate Collection Print

L10: Entry 1 of 3 File: USPT Aug 27, 2002

US-PAT-NO: 6442276
DOCUMENT-IDENTIFIER: US 6442276 B1

TITLE: Verification of authenticity of goods by use of random numbers

DATE-ISSUED: August 27, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Doljack; Frank A.	Pleasanton	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Assure Systems, Inc.	Pleasanton	CA			02

APPL-NO: 08/ 897857 [PALM]
DATE FILED: July 21, 1997

INT-CL: [07] G06 F 17/60, G09 C 3/08, H04 L 9/00, H04 L 15/34

US-CL-ISSUED: 380/51; 705/28, 713/179
US-CL-CURRENT: 380/51; 705/28, 713/179

FIELD-OF-SEARCH: 380/51, 380/55, 380/23, 705/28, 705/57, 700/215, 700/214, 713/179, 235/385

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
□	3833795	September 1974	Shoshani et al.	
□	4463250	July 1984	McNeight et al.	
□	4879747	November 1989	Leighton et al.	
□	5367148	November 1994	Storch et al.	
□	5422954	June 1995	Berson	380/51
□	5592561	January 1997	Moore	
□	5598477	January 1997	Berson	
□	5768384	June 1998	Berson	380/23
□	5818021	October 1998	Szewczykowski	235/380
□	5822739	October 1998	Kara	
□	6073114	June 2000	Perkins, III et al.	705/28
□	6105004	August 2000	Halperin et al.	705/28

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
266748	May 1988	EP	
360225	March 1990	EP	
782112	July 1997	EP	
WO 84/03019	August 1984	WO	
WO 93/22745	November 1993	WO	
WO 98 03904	January 1998	WO	

OTHER PUBLICATIONS

Tygar, J.D. et al: "Cryptographic Postage Indicia", Lecture Notes in Computer Science, Springer Verlag, New York, NY, US. vol. 1179, Dec. 1996, pp. 378-391.
"Point Of Sale Transaction Logging Scheme. Apr. 1980." IBM Technical Disclosure Bulletin, vol. 22, No. 11, Apr. 1980, pp. 5046-5049, XP002084211, New York, US.
PCT International Search Report, PCT/US98/15070, 4 pp.
Menezes, Alfred J., Paul C van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, 1997, p. 401.

ART-UNIT: 2132

PRIMARY-EXAMINER: Hayes; Gail

ASSISTANT-EXAMINER: Meislahn; Douglas

ABSTRACT:

A method of verifying the authenticity of goods includes generating one or more random codes and storing the one or more random codes in a database. The goods are then marked with one of the generated random codes such that each of the goods contain their own unique random code. Upon field checking and inventory of marked goods and comparing the codes on the marked goods to codes within the database, the authenticity of goods may be verified. Also, a system for verifying the authenticity of goods includes a database containing a plurality of unique random codes and an indication whether each of the unique random codes has been read, and a code reader or scanner for reading the code affixed to a good. The system further includes a computer apparatus or other electrical mechanism for comparing a read code to the unique random codes contained within the database such that upon comparison the comparing means indicates whether the read code is valid and if valid, whether it

has been read previously on another good, thereby indicating the good's authenticity.

68 Claims, 7 Drawing figures